Realms and Identity Policies

The following topics describe realms and identity policies:

- About Realms and Identity Policies, on page 1
- Create a Realm, on page 8
- Create an Identity Policy, on page 14
- Create an Identity Rule, on page 15
- Manage a Realm, on page 18
- Manage an Identity Policy, on page 20
- Manage an Identity Rule, on page 20

About Realms and Identity Policies

A realm consists of one or more LDAP or Microsoft Active Directory servers that share the same directory credentials. You must configure a realm to perform user and user group queries, user control, or to configure an authoritative identity source. After configuring one or more realms, you can configure an identity policy.

An identity policy associates traffic on your network with an authoritative identity source and a realm. After configuring one or more identity policies, you can associate one with an access control policy and deploy the access control policy to a managed device.

About Realms

Realms are connections between the Firepower Management Center and the user accounts on the servers you monitor. They specify the connection settings and authentication filter settings for the server. Realms can:

- Specify the users and user groups whose activity you want to monitor.
- Query the user repository for user metadata on authoritative users, as well as some non-authoritative users: POP3 and IMAP users detected by traffic-based detection and users detected by traffic-based detection, a User Agent, a TS Agent, or ISE.

You can add multiple domain controllers as directories in a realm, but they must share the same basic realm information. The directories in a realm must be exclusively LDAP or exclusively Active Directory (AD) servers. After you enable a realm, your saved changes take effect next time the Firepower Management Center queries the server.
To perform user awareness, you must configure a realm for any of the Supported Servers for Realms. The system uses these connections to query the servers for data associated with POP3 and IMAP users, and to collect data about LDAP users discovered through traffic-based detection.

The system uses the email addresses in POP3 and IMAP logins to correlate with LDAP users on an Active Directory, or OpenLDAP. For example, if a managed device detects a POP3 login for a user with the same email address as an LDAP user, the system associates the LDAP user’s metadata with that user.

To perform user control, you can configure any of the following:

- A realm for an AD server for either the User Agent or ISE
- A realm for an AD server for the TS Agent
- A realm for an AD or OpenLDAP server for captive portal

About User Download

You can configure a realm to establish a connection between the Firepower Management Center and an LDAP or AD server to retrieve user and user group metadata for certain detected users:

- LDAP and AD users authenticated by captive portal or reported by a User Agent or ISE. This metadata can be used for user awareness and user control.
- POP3 and IMAP user logins detected by traffic-based detection, if those users have the same email address as an LDAP or AD user. This metadata can be used for user awareness.

You configure LDAP server or Active Directory domain controller connections as a directory in a realm. You must check Download users and user groups for access control to download a realm's user and user group data for user awareness and user control.

The Firepower Management Center obtains the following information and metadata about each user:

- LDAP user name
- First and last names
- Email address
- Department
- Telephone number

About User Activity Data

User activity data is stored in the user activity database and user identity data is stored in the users database. The maximum number of users you can store and use in access control depends on your Firepower Management Center model. When choosing which users and groups to include, make sure the total number of users is less than your model limit. If your access control parameters are too broad, the Firepower Management Center obtains information on as many users as it can and reports the number of users it failed to retrieve in the Tasks tab page of the Message Center.
If you remove a user that has been detected by the system from your user repository, the Firepower Management Center does not remove that user from its users database; you must manually delete it. However, your LDAP changes are reflected in access control rules when the Firepower Management Center next updates its list of authoritative users.

**Realms and Trusted Domains**

When you configure a realm in the Firepower Management Center, it is associated with an Active Directory or LDAP domain.

A grouping of Microsoft Active Directory (AD) domains that trust each other is commonly referred to as a forest. This trust relationship can enable domains to access each other's resources in different ways. For example, a user account defined in domain A can be marked as a member of a group defined in domain B.

The Firepower System does not support trusted AD domains. This means that the Firepower System does not track which configured domains trust each other, and does not know which domains are parent or child domains of each other. The Firepower System also has not been tested to assure support for environments that use cross-domain trust, even when the trust relationship is exercised outside of the Firepower System.

For more information, see Troubleshoot Realms and User Downloads, on page 5.

**Supported Servers for Realms**

You can configure realms to connect to the following types of servers, providing they have TCP/IP access from the Firepower Management Center:

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Supported for User Agent data retrieval?</th>
<th>Supported for ISE data retrieval?</th>
<th>Supported for TS Agent data retrieval?</th>
<th>Supported for captive portal data retrieval?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Active Directory on Windows Server 2008 and Windows Server 2012</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OpenLDAP on Linux</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note the following about your server group configurations:

- To perform user control on user groups or on users in groups, you must configure user groups on the LDAP or Active Directory server. The Firepower Management Center cannot perform user group control if the server organizes the users in basic object hierarchy.

- Group names cannot start with `S` because it is used internally by LDAP.

Neither group names nor organizational unit names can contain special characters like asterisk (*), equals (=), or backslash (\); otherwise, users in those groups or organizational units are not downloaded and are not available for identity policies.
To configure an Active Directory realm that includes or excludes users who are members of a sub-group on your server, note that Microsoft recommends that Active Directory has no more than 5000 users per group in Windows Server 2008 or 2012. For more information, see Active Directory Maximum Limits—Scalability on MSDN.

If necessary, you can modify your Active Directory server configuration to increase this default limit and accommodate more users.

To uniquely identify the users reported by a server in your Remote Desktop Services environment, you must configure the Cisco Terminal Services (TS) Agent. When installed and configured, the TS Agent assigns unique ports to individual users so the Firepower System can uniquely identify those users. (Microsoft changed the name Terminal Services to Remote Desktop Services.)

For more information about the TS Agent, see the Cisco Terminal Services (TS) Agent Guide.

**Supported Server Object Class and Attribute Names**

The servers in your realms must use the attribute names listed in the following table for the Firepower Management Center to retrieve user metadata from the servers. If the attribute names are incorrect on your server, the Firepower Management Center cannot populate its database with the information in that attribute.

<table>
<thead>
<tr>
<th>Metadata</th>
<th>FMC Attribute</th>
<th>LDAP ObjectClass</th>
<th>Active Directory Attribute</th>
<th>OpenLDAP Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP user name</td>
<td>Username</td>
<td>user</td>
<td>samaccountname</td>
<td>cn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>inetOrgPerson</td>
<td></td>
<td>uid</td>
</tr>
<tr>
<td>first name</td>
<td>First Name</td>
<td></td>
<td>givenname</td>
<td>givenname</td>
</tr>
<tr>
<td>last name</td>
<td>Last Name</td>
<td></td>
<td>sn</td>
<td>sn</td>
</tr>
<tr>
<td>email address</td>
<td>Email</td>
<td></td>
<td>mail</td>
<td>mail</td>
</tr>
<tr>
<td>department</td>
<td>Department</td>
<td></td>
<td>department</td>
<td>ou</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>distinguishedname</td>
<td></td>
</tr>
<tr>
<td>telephone number</td>
<td>Phone</td>
<td></td>
<td>telephonenumber</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
The LDAP ObjectClass for groups is `group, groupOfNames, (group-of-names for Active Directory)` or `groupOfUniqueNames`.

For more information about ObjectClasses and attributes, see the following references:

- Microsoft Active Directory:
Troubleshoot Realms and User Downloads

If you notice unexpected server connection behavior, consider tuning your realm configuration, device settings, or server settings. For other related troubleshooting information, see:

- Troubleshoot the User Agent Identity Source
- Troubleshoot the ISE Identity Source
- Troubleshoot the TS Agent Identity Source
- Troubleshoot the Captive Portal Identity Source
- Troubleshoot User Control

Symptom: Access control policy doesn't match group membership

This solution applies to an AD domain that is in a trust relationship with other AD domains. In the following discussion, external domain means a domain other than the one to which the user logs in.

If a user belongs to a group defined in a trusted external domain, Firepower doesn't track membership in the external domain. For example, consider the following scenario:

- Domain controllers 1 and 2 trust each other
- Group A is defined on domain controller 2
- User mparvinder in controller 1 is a member of Group A

Even though user mparvinder is in Group A, the Firepower access control policy rules specifying membership Group A don't match.

Solution: Create a similar group in domain controller 1 that contains has all domain 1 accounts that belong to group A. Change the access control policy rule to match any member of Group A or Group B.

Symptom: Access control policy doesn't match child domain membership

If a user belongs to a domain that is child of parent domain, Firepower doesn't track the parent/child relationships between domains. For example, consider the following scenario:

- Domain child.parent.com is child of domain parent.com
- User mparvinder is defined in child.parent.com

Even though user mparvinder is in a child domain, the Firepower access control policy matching the parent.com don't match mparvinder in the child.parent.com domain.

Solution: Change the access control policy rule to match membership in either parent.com or child.parent.com.
**Symptom: Realm or realm directory test fails**

The **Test** button on the directory page sends an LDAP query to the hostname or IP address you entered. If it fails, check the following:

- The **Hostname** you entered resolves to the IP address of an LDAP server or Active Directory domain controller.
- The **IP Address** you entered is valid.

The **Test AD Join** button on the realm configuration page verifies the following:

- DNS resolves the **AD Primary Domain** to an LDAP server or Active Directory domain controller’s IP address.
- The **AD Join Username** and **AD Join Password** are correct.
  
  **AD Join Username** must be fully qualified (for example, `administrator@mydomain.com`, not `administrator`).

- The user has sufficient privileges to create a computer in the domain and join the Firepower Management Center to the domain as a Domain Computer.

**Symptom: User timeouts are occurring at unexpected times**

If you notice the system performing user timeouts at unexpected intervals, confirm that the time on your User Agent, ISE, or TS Agent server is synchronized with the time on the Firepower Management Center. If the appliances are not synchronized, the system may perform user timeouts at unexpected intervals.

**Symptom: Users are not included or excluded as specified in your realm configuration**

If you configure an Active Directory realm that includes or excludes users who are members of a sub-group on your server, note that Microsoft Windows servers limit the number of users they report:

- 5000 users per group on Microsoft Windows Server 2008 or 2012

If necessary, you can modify your server configuration to increase this default limit and accommodate more users.

**Symptom: Users are not downloaded**

Possible causes follow:

- If you have the realm **Type** configured incorrectly, users and groups cannot be downloaded because of a mismatch between the attribute the Firepower system expects and what the repository provides. For example, if you configure **Type** as **LDAP** for a Microsoft Active Directory realm, the Firepower system expects the **uid** attribute, which is set to **none** on Active Directory. (Active Directory repositories use **sAMAccountName** for the user ID.)

  **Solution:** Set the realm **Type** field appropriately: **AD** for Microsoft Active Directory or **LDAP** for another supported LDAP repository.

- Users in Active Directory groups that have special characters in the group or organizational unit name might not be available for identity policy rules. For example, if a group or organizational unit name contains the characters asterisk (\*), equals (=), or backslash (\), users in those groups are not downloaded and can't be used for identity policies.
Solution: Remove special characters from the group or organizational unit name.

Symptom: User data for previously-unseen ISE and User Agent users is not displaying in the web interface

After the system detects activity from an ISE, User Agent, or TS Agent user whose data is not yet in the database, the system retrieves information about them from the server. In some cases, the system requires additional time to successfully retrieve this information from Microsoft Windows servers. Until the data retrieval succeeds, activity seen by the ISE, User Agent, or TS Agent user is not displayed in the web interface.

Note that this may also prevent the system from handling the user’s traffic using access control rules.

Symptom: User data in events is unexpected

If you notice user or user activity events contain unexpected IP addresses, check your realms. The system does not support configuring multiple realms with the same AD Primary Domain value.

Symptom: Users originating from terminal server logins are not uniquely identified by the system

If your deployment includes a terminal server and you have a realm configured for one or more servers connected to the terminal server, you must deploy the Cisco Terminal Services (TS) Agent to accurately report user logins in terminal server environments. When installed and configured, the TS Agent assigns unique ports to individual users so the Firepower System can uniquely identify those users in the web interface.

For more information about the TS Agent, see the Cisco Terminal Services (TS) Agent Guide.

About Identity Policies

Identity policies contain identity rules. Identity rules associate sets of traffic with a realm and an authentication method: passive authentication, active authentication, or no authentication.

With the exception noted at the end of this topic, you must configure realms and authentication methods you plan to use before you can invoke them in your identity rules:

- You configure realms outside of your identity policy, at System > Integration > Realms. For more information, see Create a Realm, on page 8.
- You configure the User Agent and ISE, passive authentication identity sources, at System > Integration > Identity Sources. For more information, see Configure the User Agent for User Control and Configure ISE for User Control.
- You configure the TS Agent, a passive authentication identity source, outside the Firepower System. For more information, see the Cisco Terminal Services (TS) Agent Guide.
- You configure captive portal, the active authentication identity source, in the identity policy. For more information, see How to Configure the Captive Portal for User Control.

After you add multiple identity rules to a single identity policy, order the rules. The system matches traffic to rules in top-down order by ascending rule number. The first rule that traffic matches is the rule that handles the traffic.

After you configure one or more identity policies, you must associate one identity policy with your access control policy. When traffic on your network matches the conditions in your identity rule, the system associates the traffic with the specified realm and authenticates the users in the traffic using the specified identity source.

If you do not configure an identity policy, the system does not perform user authentication.
Exception to creating an identity policy

An identity policy is not required if all of the following are true:

- You use the ISE identity source.
- You do not use users or groups in access control policies.
- You use Security Group Tags (SGT) in access control policies. For more information, see ISE SGT vs Custom SGT Rule Conditions.

Related Topics

User Identity Sources

Create a Realm

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Control</td>
<td>Any</td>
<td>Any</td>
<td>Administrator, Access Admin, Network Admin</td>
</tr>
</tbody>
</table>

For more information about realm configuration fields, see Realm Fields, on page 9.

Note

You must specify a unique **AD Primary Domain** for every Microsoft Active Directory (AD) realm. Although the system allows you to specify the same **AD Primary Domain** for different AD realms, the system won't function properly. This happens because system assigns a unique ID to every user and group in each realm; therefore, the system cannot definitively identify any particular user or group.

Procedure

**Step 1** Log in to the Firepower Management Center.

**Step 2** Click **System > Integration**.

**Step 3** Click **Realms**.

**Step 4** To create a new realm, click **New Realm**.

**Step 5** To perform other tasks (such as enable, disable, or delete a realm), see Manage a Realm, on page 18.

**Step 6** Enter realm information as discussed in Realm Fields, on page 9.

**Step 7** Click **OK**.

**Step 8** Configure at least one directory as discussed in Configure a Realm Directory, on page 12.

**Step 9** Configure user and user group download (required for access control) as discussed in Download Users and Groups, on page 13.

**Step 10** Click the **Realm Configuration** tab.

**Step 11** Enter user session timeout values, in minutes, for **Authenticated Users**, **Failed Authentication Users**, and **Guest Users**.
What to do next

- Configure a Realm Directory, on page 12
- Edit, delete, enable, or disable a realm; see Manage a Realm, on page 18.
- Compare Realms, on page 19.
- Optionally, monitor the task status; see Viewing Task Messages.

Realm Fields

The following fields are used to configure a realm.

**Realm Configuration Fields**

These settings apply to all Active Directory servers or domain controllers (also referred to as directories) in a realm.

**Name**

A unique name for the realm. The system supports alphanumeric and special characters.

**Description**

(Optional.) Enter a description of the realm.

**AD Primary Domain**

For Microsoft Active Directory realms only. Domain for the Active Directory server where users should be authenticated.

---

**Note**

You must specify a unique AD Primary Domain for every Microsoft Active Directory (AD) realm. Although the system allows you to specify the same AD Primary Domain for different AD realms, the system won't function properly. This happens because system assigns a unique ID to every user and group in each realm; therefore, the system cannot definitively identify any particular user or group.

**AD Join Username and AD Join Password**

For Microsoft Active Directory realms intended for Kerberos captive portal active authentication, the distinguished username and password of any Active Directory user with appropriate rights to create a Domain Computer account in the Active Directory domain.

Keep the following in mind:

- DNS must be able to resolve the domain name to an Active Directory domain controller's IP address.
- The user you specify must be able to join computers to the Active Directory domain.
- The user name must be fully qualified (for example, administrator@mydomain.com, not administrator).

If you choose Kerberos (or HTTP Negotiate, if you want Kerberos as an option) as the Authentication Type in an identity rule, the Realm you select must be configured with an AD Join Username and AD Join Password to perform Kerberos captive portal active authentication.
**Directory Username and Directory Password**

The distinguished username and password for a user with appropriate access to the user information you want to retrieve.

Note the following:

- For Microsoft Active Directory, the user does not need elevated privileges. You can specify any user in the domain.
- For OpenLDAP, the user's access privileges are determined by the `<level>` parameter discussed in section 8 of the OpenLDAP specification. The user's `<level>` should be `auth` or better.
- The user name must be fully qualified (for example, `administrator@mydomain.com`, not `administrator`).

**Base DN**

The directory tree on the server where the Firepower Management Center should begin searching for user data.

Typically, the base distinguished name (DN) has a basic structure indicating the company domain name and operational unit. For example, the Security organization of the Example company might have a base DN of `ou=security,dc=example,dc=com`.

**Group DN**

The directory tree on the server where the Firepower Management Center should search for users with the group attribute. A list of supported group attributes is shown in Supported Server Object Class and Attribute Names, on page 4.

---

**Note**

Neither the group name nor the organizational unit name can contain special characters like asterisk (*), equals (=), or backslash (\) because users in those groups are not downloaded and cannot be used in identity policies.

**Group Attribute**

(Optional.) The group attribute for the server, `Member` or `Unique Member`.

**Type**

The type of realm, `AD` for Microsoft Active Directory or `LDAP` for other supported LDAP repositories. For a list of supported LDAP repositories, see Supported Servers for Realms, on page 3.

---

**Note**

Only captive portal supports an LDAP realm.

The following fields are available when you edit an existing realm.

**User Session Timeout**

Enter the number of minutes before user sessions time out. The default is 1440 (24 hours) after the user's login event. After the timeout is exceeded, the user's session ends; if the user continues to access the network without logging in again, the user is seen by the Firepower Management Center as Unknown.
The user session timeout values apply to both active authentication (captive portal) and passive authentication (TS Agent, user agent, ISE). Setting a large value might prevent user sessions from ending, resulting in those sessions being claimed by other users.

Note
Realm Directory Fields
These settings apply to individual servers (such as Active Directory domain controllers) in a realm.

Encryption
The encryption method to use for the Firepower Management Center-server connection:
- **STARTTLS**—encrypted LDAP connection
- **LDAPS**—encrypted LDAP connection
- **None**—unencrypted LDAP connection (unsecured traffic)

Hostname/IP Address
The host name or IP address of an Active Directory domain controller. If you specify an Encryption method, you must specify a host name in this field.

Port
The port to use for the Firepower Management Center-controller connection.

SSL Certificate
The SSL certificate to use for authentication to the server. You must configure **STARTTLS** or **LDAPS** as the Encryption type in order to use an SSL certificate.

If you are using a certificate to authenticate, the name of the server in the certificate must match the server Hostname/IP Address. For example, if you use 10.10.10.250 as the IP address but computer1.example.com in the certificate, the connection fails.

User Download Fields
Available Groups, Add to Include, Add to Exclude
Identifies the groups to download and make available for user awareness and user control.
- If you leave a group in the Available Groups box, the group is not downloaded.
- If you move a group to the Add to Include box, the group is downloaded and user data is available for user awareness and user control.
- If you move a group to the Add to Exclude box, the group name only is downloaded. Users in the group are not downloaded.
- To include users from groups that are not included, enter the user name in the field below Groups to Include and click Add.
- To exclude users from groups that are not excluded, enter the user name in the field below Groups to Exclude and click Add.
The users that are downloaded to the Firepower Management Center is calculated using the formula \( R = I - (E + e) + i \), where

- \( R \) is list of downloaded users
- \( I \) is included groups
- \( E \) is excluded groups
- \( e \) is excluded users
- \( i \) is included users

**Note**

Begin automatic download at, Repeat every

Specifies the frequency of the automatic downloads.

Download users and groups (required for user access control)

Enables you to download users and groups for user awareness and user control.

### Configure a Realm Directory

This procedure enables you to create a realm directory, which corresponds to an LDAP server or a Microsoft Active Directory domain controller. An Active Directory server can have multiple domain controllers, each of which is capable of authenticating different users and groups.

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Control</td>
<td>Any</td>
<td>Any</td>
<td>Administrator, Access Admin, Network Admin</td>
</tr>
</tbody>
</table>

For more information about realm directory configuration fields, see Realm Fields, on page 9.

**Before you begin**

To optionally use an SSL certificate to authenticate with the directory, create a certificate or have your certificate data and key available on the machine from which you're accessing the Firepower Management Center.

**Procedure**

**Step 1**

If you haven't done so already, log in to the Firepower Management Center and click Integration > Realms.

**Step 2**

On the Realms tab page, click the name of the realm for which to configure a directory.

**Step 3**


**Step 4**

Enter the Hostname / IP Address and Port for the LDAP server or Active Directory domain controller. The system sends an LDAP query to the hostname or IP address you specify. If the host name resolves to the IP address of an LDAP server or Active Directory domain controller, the Test succeeds.
Step 5: Select an Encryption Mode.

Step 6: (Optional.) Choose an SSL Certificate from the list or click the add icon (✔) to add a certificate.

Step 7: To test the connection, click Test.

Step 8: Click OK.

Step 9: Click Save. You are returned to the Realms tab page.

Step 10: If you haven’t already enabled the realm, on the Realms tab page, slide State to enabled.

What to do next
- Download Users and Groups, on page 13.

Download Users and Groups

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Control</td>
<td>Any</td>
<td>Any</td>
<td>Administrator, Access Admin, Network Admin</td>
</tr>
</tbody>
</table>

This section discusses how to download users and groups from your Active Directory server to the Firepower Management Center. If you do not specify any groups to include, the system retrieves user data for all the groups that match the parameters you provided. For performance reasons, Cisco recommends that you explicitly include only the groups that represent the users you want to use in access control.

The maximum number of users the Firepower Management Center can retrieve from the server depends on your Firepower Management Center model. If the download parameters in your realm are too broad, the Firepower Management Center obtains information on as many users as it can and reports the number of users it failed to retrieve in the Task tab of the Message Center.

User names that include Unicode characters do not display in the Firepower Management Center. Before you download users and groups, make sure to replace Unicode characters with alphanumeric characters.

For more information about realm configuration fields, see Realm Fields, on page 9.

Procedure

Step 1: Log in to the Firepower Management Center.

Step 2: Click System > Integration > Realms.

Step 3: To download users and groups manually, click the download icon (✔) next to the realm to download users and user groups. If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration. You can skip the remainder of this procedure.

Step 4: To configure the realm for automatic user and group download, click the edit icon (✍) next to the realm to configure for automatic user and group download.
Step 5 On the User Access Control tab page, check **Download users and groups (required for user access control)**.

Step 6 Select a time to **Begin automatic download at** from the lists.

Step 7 Select a download interval from the **Repeat Every** list.

Step 8 To include or exclude user groups from the download, choose user groups from the **Available Groups** column and click **Add to Include** or **Add to Exclude**.

Separate multiple users with commas. You can also use an asterisk (\*) as a wildcard character in this field.

**Note** You must **Add to Include** if you want to perform user control on users in that group.

Use the following guidelines:

- If you leave a group in the **Available Groups** box, the group is not downloaded.
- If you move a group to the **Add to Include** box, the group is downloaded and user data is available for user awareness and user control.
- If you move a group to the **Add to Exclude** box, the group is downloaded and user data is available for user awareness, but not for user control.
- To include users from groups that are not included, enter the user name in the field below **Groups to Include** and click **Add**.
- To exclude users from groups that are not excluded, enter the user name in the field below **Groups to Exclude** and click **Add**.

---

**Create an Identity Policy**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Control</td>
<td>Any</td>
<td>Any</td>
<td>Administrator, Access Admin, Network Admin</td>
</tr>
</tbody>
</table>

**Before you begin**

An identity policy is required to use users and groups in a realm in access control policies. Create and enable one or more realms as described in **Create a Realm, on page 8**.

An identity policy is not required if all of the following are true:

- You use the ISE identity source.
- You do not use users or groups in access control policies.
- You use Security Group Tags (SGT) in access control policies. For more information, see **ISE SGT vs Custom SGT Rule Conditions**.
### Create an Identity Rule

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Control</td>
<td>Any</td>
<td>Any</td>
<td>Administrator, Access Admin, Network Admin</td>
</tr>
</tbody>
</table>

For details about configuration options for identity rules, see [Identity Rule Fields, on page 16](#).

#### Procedure

**Step 1** If you haven't done so already, log in to the Firepower Management Center.

**Step 2** Click Policies > Access Control > Identity.

**Step 3** Click edit (📝) next to the identity policy to which to add the identity rule.

If a view icon (🔍) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 4** Click Add Rule.
**Step 5** Enter a **Name**.

**Step 6** Specify whether the rule is **Enabled**.

**Step 7** To add the rule to an existing category, indicate where you want to **Insert** the rule. To add a new category, click **Add Category**.

**Step 8** Choose a rule **Action** from the list.

**Step 9** Click the **Realms & Settings** tab.

**Step 10** Choose a realm for the identity rule from the **Realms** list. You must associate a realm with every identity rule.

The only exception to the realm requirement is implementing user control using only the ISE SGT attribute tag. In this case, you do not need to configure a realm for the ISE server. ISE SGT attribute conditions can be configured in policies with or without an associated identity policy.

**Step 11** If you're configuring captive portal, see **How to Configure the Captive Portal for User Control**.

**Step 12** (Optional) To add conditions to the identity rule, see **Rule Condition Types**.

**Step 13** Click **Add**.

**Step 14** In the policy editor, set the rule position. Click and drag or use the right-click menu to cut and paste. Rules are numbered starting at 1. The system matches traffic to rules in top-down order by ascending rule number. The first rule that traffic matches is the rule that handles that traffic. Proper rule order reduces the resources required to process network traffic and prevents rule preemption.

**Step 15** Click **Save**.

---

**Related Topics**

- **Snort® Restart Scenarios**

---

**Identity Rule Fields**

Use the following fields to configure identity rules.

**Enabled**

Choosing this option enables the identity rule in the identity policy. Deselecting this option disables the identity rule.

**Action**

Specify the type of authentication you want to perform on the users in the specified realm: **Passive Authentication** (default), **Active Authentication**, or **No Authentication**. You must fully configure the authentication method, or **identity source**, before selecting it as the action in an identity rule.

---

**Caution**

Adding the first or removing the last active authentication rule when SSL decryption is disabled (that is, when the access control policy does not include an SSL policy) restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See **Snort® Restart Traffic Behavior** for more information.

Note that an active authentication rule has either an **Active Authentication** rule action, or a **Passive Authentication** rule action with **Use active authentication if passive authentication cannot identify user** selected.
For information about which passive and active authentication methods are supported in your version of the Firepower System, see About User Identity Sources.

**Realm**

The realm containing the users you want to perform the specified Action on. You must fully configure a realm before selecting it as the realm in an identity rule.

**Note**

If you select Kerberos (or HTTP Negotiate, if you want Kerberos as an option) as the Authentication Type for the identity rule, the Realm you select must be configured with an AD Join Username and AD Join Password to perform Kerberos captive portal active authentication.

**Use active authentication if passive authentication cannot identify user**

Selecting this option authenticates users using captive portal active authentication if a passive or a VPN authentication fails to identify them. You must configure captive portal active authentication in your identity policy in order to select this option.

If you disable this option, users that do not have a VPN identity or that passive authentication cannot identify are identified as Unknown.

**Identify as Special Identities/Guest if authentication cannot identify user**

This field is displayed only if you configure Active Authentication (that is, captive portal authentication) as the rule Action.

**Authentication Type**

The method to use to perform captive portal active authentication. The selections vary depending on the type of realm, LDAP or AD:

- Choose HTTP Basic if you want to authenticate users using an unencrypted HTTP Basic Authentication (BA) connection. Users log in to the network using their browser's default authentication popup window.

  Most web browsers cache the credentials from HTTP Basic logins and use the credentials to seamlessly begin a new session after an old session times out.

- Choose NTLM to authenticate users using a NT LAN Manager (NTLM) connection. This selection is available only when you select an AD realm. If transparent authentication is configured in a user's browser, the user is automatically logged in. If transparent authentication is not configured, users log in to the network using their browser's default authentication popup window.

- Choose Kerberos to authenticate users using a Kerberos connection. This selection is available only when you select an AD realm for a server with secure LDAP (LDAPS) enabled. If transparent authentication is configured in a user's browser, the user is automatically logged in. If transparent authentication is not configured, users log in to the network using their browser's default authentication popup window.

**Note**

The Realm you select must be configured with an AD Join Username and AD Join Password to perform Kerberos captive portal active authentication.
If you are creating an identity rule to perform Kerberos captive portal and you have DNS resolution configured, you must configure your DNS server to resolve the fully qualified domain name (FQDN) of the captive portal device. The FQDN must match the host name you provided when configuring DNS.

For ASA with FirePOWER Services and Firepower Threat Defense devices, the FQDN must resolve to the IP address of the routed interface used for captive portal.

- Choose **HTTP Negotiate** to allow the captive portal server to choose between HTTP Basic, Kerberos, or NTLM for the authentication connection. This type is available only when you select an AD realm.

The **Realm** you choose must be configured with an **AD Join Username** and **AD Join Password** for **HTTP Negotiate** to choose Kerberos captive portal active authentication.

If you are creating an identity rule to perform **HTTP Negotiate** captive portal and you have DNS resolution configured, you must configure your DNS server to resolve the fully qualified domain name (FQDN) of the captive portal device. The FQDN of the device you are using for captive portal must match the hostname you provided when configuring DNS.

For ASA with FirePOWER Services devices, the FQDN is the FQDN of the ASA FirePOWER module.

## Manage a Realm

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Control</td>
<td>Any</td>
<td>Any</td>
<td>Administrator, Access Admin, Network Admin</td>
</tr>
</tbody>
</table>

This section discusses how to perform various maintenance tasks for a realm using controls on the Realms page. Note the following:

- If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

- If a view icon (-gay) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
Procedure

Step 1 Log in to the Firepower Management Center.
Step 2 Click System > Integration.
Step 3 Click Realms.
Step 4 To delete a realm, click the delete icon ( DELETE ).
Step 5 To edit a realm, click the edit icon ( EDIT ) next to the realm and make changes as described in Create a Realm, on page 8.
Step 6 To enable a realm, slide State to the right; to disable a realm, slide it to the left.
Step 7 To download users and user groups, click the download icon ( DOWNLOAD ).
Step 8 To copy a realm, click the copy icon ( COPY ).
Step 9 To compare realms, see Compare Realms, on page 19.

Compare Realms

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Control</td>
<td>Any</td>
<td>Any</td>
<td>Administrator, Security Approver, Access Admin, Network Admin</td>
</tr>
</tbody>
</table>

Procedure

Step 1 Log in to the Firepower Management Center.
Step 2 Click System > Integration.
Step 3 Click Realms.
Step 4 Click System > Integration.
Step 5 Click Realms.
Step 6 Click Compare Realms.
Step 7 Choose Compare Realm from the Compare Against list.
Step 8 Choose the realms you want to compare from the Realm A and Realm B lists.
Step 9 Click OK.
Step 10 To navigate individually through changes, click Previous or Next above the title bar.
Step 11 (Optional.) Click Comparison Report to generate the realm comparison report.
Step 12 (Optional.) Click New Comparison to generate a new realm comparison view.
Manage an Identity Policy

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Control</td>
<td>Any</td>
<td>Any</td>
<td>Administrator, Access Admin, Network Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.

Procedure

**Step 1**  
If you haven't done so already, log in to the Firepower Management Center.

**Step 2**  
Click Policies > Access Control > Identity.

**Step 3**  
To delete a policy, click delete (-trash). If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 4**  
To edit a policy, click edit (-pencil) next to the policy and make changes as described in Create an Identity Policy, on page 14. If a view icon (-eye) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 5**  
To copy a policy, click the copy icon (-clone).

**Step 6**  
To generate a report for the policy, click the report icon (-report) as described in Generating Current Policy Reports.

**Step 7**  
To compare policies, see Comparing Policies.

Manage an Identity Rule

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Control</td>
<td>Any</td>
<td>Any</td>
<td>Administrator, Access Admin, Network Admin</td>
</tr>
</tbody>
</table>

Procedure

**Step 1**  
If you haven't already done so, log in to the Firepower Management Center.

**Step 2**  
Click Policies > Access Control > Identity.
Step 3  Click the edit icon (📝) next to the policy you want to edit. If a view icon (👀) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4  To edit an identity rule, click the edit icon (📝) and make changes as described in Create an Identity Policy, on page 14.

Step 5  To delete an identity rule, click the delete icon (🗑️).

Step 6  To create a rule category, click Add Category and choose the position and the rule.

Step 7  Click Save.

What to do next

• Deploy configuration changes; see Deploy Configuration Changes.
Manage an Identity Rule